Algebraic Number Theory

Swayam Chube

January 4, 2025

Contents

§1 Algebraic Integers

§§ Integrality

Definition 1.1. The *discriminant* of a basis $\alpha_1, \ldots, \alpha_n$ of a separable extension L/K of degree n is defined by

$$d(\alpha_1, \ldots, \alpha_n) = \det\left((\sigma_i \alpha_j)\right)^2$$

where σ_i, $i = 1, \ldots, n$ are the distinct K-embeddings of L into $\overline{K}$.

It is not hard to see that

$$d(\alpha_1, \ldots, \alpha_n) = \det\left((\mathrm{Tr}_K^L(\alpha_i \alpha_j))\right).$$

Proposition 1.2. If L/K is a finite separable field extension and $\alpha_1, \ldots, \alpha_n$ is a K-basis for L, then the discriminant

$$d(\alpha_1, \ldots, \alpha_n) \neq 0,$$

and the *trace pairing* $(x, y) = \mathrm{Tr}_K^L(xy)$ is a nondegenerate bilinear form on the K-vector space L.

Proof. We first show that the trace pairing is nondegenerate. Let $\theta \in L$ be a primitmive element. Then, a K-basis for L is given by $\{1, \theta, \ldots, \theta^{n-1}\}$. With respect to this basis, the trace pairing is represented by the matrix $M = \left((\mathrm{Tr}_K^L(\theta^{i-1}\theta^{j-1}))\right)$ which is a Vandermonde matrix and hence, has nonzero determinant. Thus, the trace pairing is nondegenerate.

Next, consider L with the basis $\{\alpha_1, \ldots, \alpha_n\}$. The matrix of the trace pairing with respect to this basis is $\left((\mathrm{Tr}_K^L(\alpha_i \alpha_j))\right)$ and must have nonzero determinant. It follows that $d(\alpha_1, \ldots, \alpha_n) \neq 0$. ∎

Notation. Henceforth, let A be an integrally closed domain with fraction field K, L a finite separable extension of L, and B the integral closure of A in L.

Lemma 1.3. Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L which is contained in B, of discriminant $d = d(\alpha_1, \ldots, \alpha_n)$. Then one has

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Proof. Let $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in B$ with $a_i \in K$ for $1 \leqslant i \leqslant n$. Consider the matrix equation

$$\begin{pmatrix} & \vdots & \\ \cdots & \mathrm{Tr}_K^L(\alpha_i \alpha_j) & \cdots \\ & \vdots & \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_K^L(\alpha_1 \alpha) \\ \vdots \\ \mathrm{Tr}_K^L(\alpha_n \alpha). \end{pmatrix}$$

The matrix has elements in A and hence, its inverse is some matrix with elements in A divided by its determinant, which is d. Thus, each a_i is in $\frac{1}{d}A$ and the conclusion follows. ∎

Definition 1.4. A system of elements $\omega_1, \ldots, \omega_n \in B$ such that each $b \in B$ can be written uniquely as a linear combination

$$b = a_1\omega_1 + \cdots + a_n\omega_n$$

with coefficients $a_i \in A$ is called an *integral basis* of B over A.

Remark 1.5. The existence of an integral basis signifies that B is a free A-module of rank n and this may not always be true. Therefore, an integral basis may not always exist.

Proposition 1.6. If in addition to our setup, A is a PID, then every finitely generated B-submodule $M \neq 0$ of L is a free A-module of rank $n = [L : K]$. In particular, B admits an integral basis over A.

Proof. add in ■

§§ Dedekind Domains

Definition 1.7. A noetherian, integrally closed domain of Krull dimension 1 is called a *Dedekind domain*.

We shall now prove that ideals in a Dedekind domain admit unique factorization. Let $\mathfrak{o}$ be a Dedekind domain.

Lemma 1.8. For every ideal $\mathfrak{a} \neq 0$ of $\mathfrak{o}$, there exist nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.

Proof. Let $\mathfrak{M}$ be the colection of all ideals that do not fulfill this condition. Suppose $\mathfrak{M}$ is nonempty. Thus, it contains a maximal element, say $\mathfrak{a}$, which cannot be a prime ideal, so there exist $b_1, b_2 \in \mathfrak{o} \setminus \mathfrak{a}$ such that $b_1b_2 \in \mathfrak{a}$. Let $\mathfrak{a}_1 = \mathfrak{a} + (b_1)$ and $\mathfrak{a}_2 = \mathfrak{a} + (b_2)$. The maximality of $\mathfrak{a}$ forces $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathfrak{M}$. Further, note that $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a} + (b_1b_2) = \mathfrak{a}$, whence $\mathfrak{a} \in \mathfrak{M}$, a contradiction. ■

Lemma 1.9. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$ and set

$$\mathfrak{p}^{-1} = \{x \in K \colon x\mathfrak{p} \subseteq \mathfrak{o}\}.$$

Then one has $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ or every ideal $\mathfrak{a} \neq 0$.

Proof. First, we show that $\mathfrak{p}^{-1} \neq \mathfrak{o}$. Let $0 \neq a \in \mathfrak{p}$ and $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$, with r the minimal such. Due to prime avoidance, $\mathfrak{p}_i = \mathfrak{p}$ for some $1 \leqslant i \leqslant n$. Without loss of generality, let $\mathfrak{p} = \mathfrak{p}_1$. Since $\mathfrak{p}_2 \cdots \mathfrak{p}_n \subsetneq (a)$, choose $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a)$, equivalently, $a^{-1}b \notin \mathfrak{o}$. But on the other hand, we have $b\mathfrak{p} \subseteq (a)$ whence $a^{-1}b\mathfrak{p} \subseteq \mathfrak{o}$, consequently, $a^{-1}b \in \mathfrak{p}^{-1}$. It follows that $\mathfrak{p} \neq \mathfrak{o}$.

Now, let $\mathfrak{a} \neq 0$ be an ideal of $\mathfrak{o}$ and let $\alpha_1, \ldots, \alpha_n$ be a generating set for $\mathfrak{a}$. Assume that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ and choose $x \in \mathfrak{p}^{-1} \setminus \mathfrak{o}$. We can write

$$x\alpha_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in \mathfrak{o}.$$

Let A denote the matrix $\left(x\delta_{ij} - a_{ij}\right)$ to obtain

$$A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0.$$

Multiplying with the adjugate, we get $\det(A)\alpha_i = 0$ for $1 \leqslant i \leqslant n$. Since we are in an integral domain and $\mathfrak{a} \neq 0$, this forces $\det(A) = 0$, consequently, x is integral over $\mathfrak{o}$, a contradiction to $\mathfrak{o}$ being integrally closed. ■

THEOREM 1.10. Every ideal $\mathfrak{a}$ of $\mathfrak{o}$ different from (0) and (1) admits a factorization $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ into nonzero prime ideals $\mathfrak{p}_i$ of $\mathfrak{o}$ which is unique up to the order of the factors.

Proof. **Existence.** Let $\mathfrak{M}$ be the collection of all ideals different from (0) and (1) that do not admit a factorization. Suppose $\mathfrak{M}$ is nonempty and choose a maximal element $\mathfrak{a}$ in it. There is a maximal ideal $\mathfrak{p}$ containing $\mathfrak{a}$ and we have

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{o}.$$

Also note that $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{o}$ and hence $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$. Now note that $\mathfrak{a}\mathfrak{p}^{-1}$ is an ideal in $\mathfrak{o}$ and since $\mathfrak{a} \neq \mathfrak{p}$, this ideal must be proper. Thus, it admits a prime decomposition which when multiplied by $\mathfrak{p}$ gives a prime decomposition of $\mathfrak{a}$, a contradiction.
Uniqueness. Suppose

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Due to prime avoidance, for every $1 \leqslant i \leqslant s$, there is an index j such that $\mathfrak{p}_j = \mathfrak{q}_i$. Multiplying both sides by $\mathfrak{p}_j^{-1}$, we obtain a smaller decomposition. Now induct downwards. ■

DEFINITION 1.11. Let $\mathfrak{o}$ be a Dedekind domain with fraction field K. A *fractional ideal* of K is a finitely generated $\mathfrak{o}$-submodule $\mathfrak{a} \neq 0$ of K.

REMARK 1.12. Note that every ideal of $\mathfrak{o}$ is a fractional ideal and conversely, every fractional ideal contained in $\mathfrak{o}$ is an ideal. To belabour the point, we shall call the ideals contained in $\mathfrak{o}$ as *integral ideals*.

PROPOSITION 1.13. The fractional ideals form an abelian group, the *ideal group* J_K of K. The identity element is $(1) = \mathfrak{o}$, and the inverse of $\mathfrak{a}$ is

$$\mathfrak{a}^{-1} = \{x \in K \colon x\mathfrak{a} \subseteq \mathfrak{o}\}.$$

Proof. We have argued in the preceding proof that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$. To see that $\mathfrak{p}^{-1}$ is a fractional ideal, choose any $0 \neq d \in \mathfrak{p}$. Then $d\mathfrak{p}^{-1} \subseteq \mathfrak{o}$ and the conclusion follows.

Hence, for any integral ideal $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, we have an inverse given by $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$, which is a fractional ideal. Since $\mathfrak{b}\mathfrak{a} = \mathfrak{o}$, we have that $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Conversely, if $x \in \mathfrak{a}^{-1}$, then $x\mathfrak{o} = x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{o}\mathfrak{b} \subseteq \mathfrak{b}$, that is, $x \in \mathfrak{b}$ and hence, $\mathfrak{b} = \mathfrak{a}^{-1}$. This completes the proof. ■

COROLLARY 1.14. Every fractional ideal $\mathfrak{a} \neq 0$ admits a unique representation as a product

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}$$

with $v_{\mathfrak{p}} \in \mathbb{Z}$ and $v_{\mathfrak{p}} = 0$ almost everywhere.

Proof. There is a $d \neq 0$ in $\mathfrak{o}$ such that $d\mathfrak{a} \subseteq \mathfrak{o}$ and hence, admits a prime decomposition $d\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Also, since (d) admits a prime decomposition, dividing the two, the conclusion follows. ■

DEFINITION 1.15. The fractional ideals of the form $(a) = a\mathfrak{o}$ where $a \in K$ are called the principal fractional ideals. The principal fractional ideals corresponding to elements of $K^\times$ form a subgroup of J_K denoted by P_K. The quotient $\mathrm{Cl}_K = J_K/P_K$ is called the *ideal class group*.

PROPOSITION 1.16. Let $0 \neq \mathfrak{a}$ be an integral ideal of a Dedekind domain $\mathfrak{o}$. Then $\mathfrak{o}/\mathfrak{a}$ is a principal ring.

Proof. Due to the Chinese Remainder Theorem, it suffices to prove this for $\mathfrak{a} = \mathfrak{p}^n$ where $\mathfrak{p}$ is a maximal ideal and n a positive integer. Choose some $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ and let $1 \leqslant k \leqslant n$. Consider the decomposition of $\pi\mathfrak{o} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Since $\mathfrak{p} \supseteq \mathfrak{p}$, exactly one of the $\mathfrak{p}_i$'s must be equal to $\mathfrak{p}$. Hence, we can write $\pi\mathfrak{o} = \mathfrak{p}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal comaximal with $\mathfrak{p}$. Thus,

$$\frac{\pi\mathfrak{o}}{\mathfrak{p}^n} = \frac{\mathfrak{p}\mathfrak{a} + \mathfrak{p}^n}{\mathfrak{p}^n} = \frac{\mathfrak{p}}{\mathfrak{p}^n}$$

is principal. Further, since every ideal of $\mathfrak{o}/\mathfrak{p}^n$ is of the form $\mathfrak{p}^k/\mathfrak{p}^n$, the conclusion follows. ■

COROLLARY 1.17. Every ideal of a Dedekind domain can be generated by two elements.

Proof. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{o}$ and choose $0 \neq a \in \mathfrak{a}$. Then, $\mathfrak{a}/(a)$ is principal in $\mathfrak{o}/(a)$ and the conclusion follows. ■

PROPOSITION 1.18. A Dedekind domain with finitely many prime ideals is a PID.

Proof. It suffices to show that all maximal ideals are principal. Let $\mathfrak{p}$ be a maximal ideal. Let $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Using the Chinese Remainder Theorem, choose some $x \in \mathfrak{o}$ with

$$x \equiv \pi \pmod{\mathfrak{p}^2} \quad \text{and} \quad x \equiv 1 \pmod{\mathfrak{q}},\ \mathfrak{q} \neq \mathfrak{p}.$$

It is easy to see that $(x) = \mathfrak{p}$ thereby completing the proof. ■

PROPOSITION 1.19. Let A be an integral domain. Every invertible fractional ideal of A is projective.

Proof. Let $\mathfrak{a}$ be an invertible fractional ideal of A and set $\mathfrak{b} = \mathfrak{a}^{-1}$. By definition, there are $x_1, \ldots, x_n \in \mathfrak{a}$, and $y_1, \ldots, y_n \in \mathfrak{b}$ such that $x_1y_1 + \cdots + x_ny_n = 1$. Hence, for any $x \in \mathfrak{a}$,

$$x = x_1(y_1x) + \cdots + x_n(y_nx),$$

but $y_1x, \ldots, y_nx \in \mathfrak{b}\mathfrak{a} = A$, whence $\mathfrak{a} \subseteq Ax_1 + \cdots + Ax_n \subseteq \mathfrak{a}$, that is, $\mathfrak{a} = Ax_1 + \cdots + Ax_n$. Similarly, one can show that $\mathfrak{b} = Ay_1 + \cdots + Ay_n$.

Now, let $M \twoheadrightarrow \mathfrak{a}$ be a surjective A-linear map. Choose $m_i \in M$ such that $f(m_i) = x_i$ for $1 \leqslant i \leqslant n$, and define $g : \mathfrak{a} \to M$ by

$$g(x) = \sum_{i=1}^{n} (xy_i)m_i,$$

which is well-defined because $xy_i \in \mathfrak{a}\mathfrak{b} = A$. Then,

$$f(g(x)) = \sum_{i=1}^{n} (xy_i)f(m_i) = \sum_{i=1}^{n} (xy_i)x_i = x,$$

which completes the proof. ∎

§§ Extensions of Dedekind Domains

LEMMA 1.20. Let $\mathfrak{o}$ be a noetherian domain of dimension 1 and $\widetilde{\mathfrak{o}}$ its integral closure. Then, for each ideal $\mathfrak{a} \neq 0$ of $\mathfrak{o}$, the quotient $\widetilde{\mathfrak{o}}/\mathfrak{a}\widetilde{\mathfrak{o}}$ is a finitely generated $\mathfrak{o}$-module.

Proof. Let $0 \neq a \in \mathfrak{a}$. Then $\widetilde{\mathfrak{o}}/\mathfrak{a}\widetilde{\mathfrak{o}}$ is a quotient of $\widetilde{\mathfrak{o}}/a\widetilde{\mathfrak{o}}$ and hence, it suffices to show that the latter is a finitely generated $\mathfrak{o}$-module. To this end, set

$$\mathfrak{a}_m = \left(a^m\widetilde{\mathfrak{o}} \cap \mathfrak{o}, a\mathfrak{o}\right).$$

This is a descending chain of ideals containing $a\mathfrak{o}$. Note that $\mathfrak{o}/a\mathfrak{o}$ is a dim 0 noetherian ring, i.e., is artinian. Hence, the chain $\mathfrak{a}_m$ must be stationary. Let n be an index such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$.

We contend that $\widetilde{\mathfrak{o}} \subseteq a^{-n}\mathfrak{o} + a\widetilde{\mathfrak{o}}$. Let $\beta = \frac{b}{c} \in \widetilde{\mathfrak{o}} \setminus \{0\}$ with $b, c \in \mathfrak{o}$. Again, note that $\mathfrak{o}/c\mathfrak{o}$ is artinian and hence, the chain of ideals $(\overline{a}^m)$ where $\overline{a} = a \bmod c\mathfrak{o}$ stabilizes. Then, there is a smallest positive integer h such that $(\overline{a}^h) = (\overline{a}^{h+1}) = \cdots$.

In particular, we can find some $x \in \mathfrak{o}$ such that $a^h \equiv xa^{h+1} \bmod c\mathfrak{o}$, that is, $a^h(1 - xa) \in c\mathfrak{o}$. Therefore,

$$\beta = \frac{b}{c}(1 - xa) + \beta xa = \frac{b}{a^h}\frac{(1 - xa)a^h}{c} + \beta xa \in a^{-h}\mathfrak{o} + a\widetilde{\mathfrak{o}}.$$

Let h be the smallest positive integer such that $\beta \in a^{-h}\mathfrak{o} + a\widetilde{\mathfrak{o}}$. It suffices to show that $h \leqslant n$. Suppose to the contrary that $h > n$. We can then write

$$\beta = \frac{u}{a^h} + a\widetilde{u} \quad \text{where } u \in \mathfrak{o},\ \widetilde{u} \in \widetilde{\mathfrak{o}}.$$

Hence, $u = a^h(\beta - a\widetilde{u}) \in a^h\widetilde{\mathfrak{o}} \cap \mathfrak{o} \subseteq \mathfrak{a}_h = \mathfrak{a}_{h+1}$ since $h > n$. Hence, $u = a^{h+1}\widetilde{u}' + au'$ for some $\widetilde{u}' \in \widetilde{\mathfrak{o}}$ and $u' \in \mathfrak{o}$. Substituting this back into the expression for β, we have

$$\beta = a\widetilde{u}' + \frac{u'}{a^{h-1}} + a\widetilde{u}' \in a^{-(h-1)}\mathfrak{o} + a\widetilde{\mathfrak{o}},$$

a contradiction to the minimality of h. Thus, we have $\widetilde{\mathfrak{o}} \subseteq a^{-n}\mathfrak{o} + a\widetilde{\mathfrak{o}}$.

Hence, $\widetilde{\mathfrak{o}}/a\widetilde{\mathfrak{o}}$ becomes a submodule of the $\mathfrak{o}$-module $(a^{-n}\mathfrak{o} + a\widetilde{\mathfrak{o}})/a\widetilde{\mathfrak{o}}$ which is generated by a^{-n} mod $a\widetilde{\mathfrak{o}}$. It is therefore a finitely generated $\mathfrak{o}$-module, thereby completing the proof. ■

THEOREM 1.21 (KRULL-AKIZUKI). Let $\mathfrak{o}$ be a one-dimensional noetherian integral domain with fraction field K. Let L/K be a finite extension and $\mathfrak{O}$ the integral closure of $\mathfrak{o}$ in L. Then $\mathfrak{O}$ is a Dedekind domain.

Proof. Let $\omega_1, \ldots, \omega_n \in \mathfrak{O}$ be a K-basis of L and let $\mathfrak{O}_0 = \mathfrak{o}[\omega_1, \ldots, \omega_n]$, which is a one-dimensional noetherian ring. Note that $\mathfrak{O}$ is the integral closure of $\mathfrak{O}_0$.

Let $\mathfrak{A}$ be an ideal of $\mathfrak{O}$. We shall show that $\mathfrak{A}$ is a finitely generated $\mathfrak{O}$-module. Choose some $0 \neq a \in \mathfrak{A} \cap \mathfrak{O}_0$ (it is an easy exercise to see that such an element exists). By the preceding lemma, $\mathfrak{O}/a\mathfrak{O}$ is a finitely generated $\mathfrak{O}_0$-module, whence is noetherian. Thus, it is also a noetherian $\mathfrak{O}$-module. Consequently, the submodule $\mathfrak{A}/a\mathfrak{O}$ is also a noetherian $\mathfrak{O}$-module, whence $\mathfrak{A}$ is a noetherian $\mathfrak{O}$-module. This completes the proof. ■

DEFINITION 1.22. Let $\mathfrak{o}$ be a Dedekind domain with fraction field K, L a finite extension of K and $\mathfrak{O}$ the integral closure of $\mathfrak{o}$ in L. If $\mathfrak{p}$ is a maximal in $\mathfrak{o}$, then there is a prime decomposition

$$\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

where the exponent e_i is called the *ramification index* and the degree of the field extension $f_i = [\mathfrak{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}]$ is called the *inertia degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$.

REMARK 1.23. Note that a prime $\mathfrak{P}$ lies over $\mathfrak{p}$ if and only if $e(\mathfrak{P}/\mathfrak{p}) \geqslant 1$.

THEOREM 1.24. Let L/K be finite separable. Then we have the *fundamental identity*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Proof. ■

§2 MINKOWSKI AND DIRICHLET'S THEOREMS

§§ Minkowski's Bound

Let K be a number field, and $\mathfrak{o}$ be its ring of integers, i.e., the integral closure of $\mathbb{Z}$ in K. We have seen that $\mathfrak{o}$ is a Dedekind domain, and hence, the group of fractional ideals is a free abelian group with basis given by the integral prime ideals of $\mathfrak{o}$. In this section, we shall show that the class group, which is the quotient of the group of fractional ideals by the principal fractional ideals, is finite. Further, we shall also obtain bounds on the ideals representing each ideal class in the class group, $\mathrm{Cl}\, K$.

THEOREM 2.1. There is a $\lambda > 0$ (depending on K) such that for every non-zero ideal $\mathfrak{a}$ of $\mathfrak{o}$, there is an $\alpha \in \mathfrak{a} \setminus \{0\}$ such that

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| \leqslant \lambda \mathfrak{N}(\mathfrak{a}).$$

Proof. Let $n = [K : \mathbb{Q}]$, and $\{\alpha_1, \ldots, \alpha_n\}$ an integral basis of $\mathfrak{o}$ as a $\mathbb{Z}$-module, and $\{\sigma_1, \ldots, \sigma_n\}$ the distinct embeddings of K into $\mathbb{C}$. Set

$$\lambda = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\sigma_i \alpha_j| \right).$$

Let m be the unique positive integer such that $m^n \leqslant \mathfrak{N}(\mathfrak{a}) < (m+1)^n$ and consider $(m+1)^n$ distinct elements of the form

$$\sum_{i=1}^{n} m_i \alpha_i \qquad \text{where} \quad 0 \leqslant m_i \leqslant m.$$

Since $[\mathfrak{o} : \mathfrak{a}] = \mathfrak{N}(\mathfrak{a}) < (m+1)^n$, two of the above must be the same modulo $\mathfrak{a}$. Thus, there is an

$$\alpha = \sum_{i=1}^{n} m_i \alpha_i \qquad -m \leqslant m_i \leqslant m$$

with $\alpha \in I$. Now, note that

$$\begin{aligned} \left|N_{\mathbb{Q}}^{K}(\alpha)\right| &= \prod_{i=1}^{n} \left| \sum_{j=1}^{n} m_j \sigma_i(\alpha_j) \right| \\ &\leqslant \prod_{i=1}^{n} \left(m \sum_{j=1}^{n} |\sigma_i(\alpha_j)| \right) \\ &\leqslant \lambda \cdot m^n \leqslant \lambda \mathfrak{N}(\mathfrak{a}), \end{aligned}$$

thereby completing the proof. ■

COROLLARY 2.2. In addition to the conclusion of the theorem, every ideal class in $\mathrm{Cl}(K)$ contains an integral ideal $\mathfrak{a}$ with $\mathfrak{N}(\mathfrak{a}) \leqslant \lambda$.

Proof. Let $C \in \mathrm{Cl}(K)$ be an ideal class. If $C = 0$, then there is nothing to prove. Else, lt $\mathfrak{b}$ be an integral ideal in the ideal class C^{-1}. According to the theorem, there is an $\alpha \in \mathfrak{b}$ such that $|N_{\mathbb{Q}}^{K}(\alpha)| \leqslant \lambda \mathfrak{N}(\mathfrak{b})$. Due to unique factorization, we can find an integral ideal $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{b} = (\alpha)$. Since $\mathfrak{b} \in C^{-1}$, we have that $\mathfrak{a} \in C$. Further,

$$\lambda \mathfrak{N}(\mathfrak{b}) \geqslant \left|N_{\mathbb{Q}}^{K}(\alpha)\right| = \mathfrak{N}(\alpha\mathfrak{o}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}) \implies \mathfrak{N}(\mathfrak{a}) \leqslant \lambda,$$

which completes the proof. ■

COROLLARY 2.3. $\mathrm{Cl}(K)$ is a finite group.

Proof. Due to the preceding result, every ideal class in $\mathrm{Cl}(K)$ has an integral ideal $\mathfrak{a}$ representing it with $\mathfrak{N}(\mathfrak{a}) \leqslant \lambda$. There is a prime factorization

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \implies \mathfrak{N}(\mathfrak{a}) = \prod_{i=1}^{r} \mathfrak{N}(\mathfrak{p}_i)^{e_i}.$$

Note that if $\mathfrak{p}_i \cap \mathbb{Z} = p_i\mathbb{Z}$, then $\mathfrak{N}(\mathfrak{p}_i) \geqslant p_i$. In particular, we have $\lambda \geqslant p_1^{e_1} \cdots p_r^{e_r}$. Thus, the $\mathfrak{p}_i$'s which occur in the decomposition of $\mathfrak{a}$ can lie over only those rational primes which are less than λ. Futher, for each $\mathfrak{p}$ lying over a rational prime p, the exponent e of $\mathfrak{p}$ in the decomposition of $\mathfrak{a}$ is bounded. Thus, $\mathfrak{a}$ has only finitely many possible prime decompositions. It follows that $\mathrm{Cl}(K)$ is finite. ∎

Our next goal is to establish "Minkowski's bound". Let K be a number field with $[K : \mathbb{Q}] = n$ and $\mathfrak{o} \subseteq K$ the ring of integers. Let $\sigma_1, \ldots, \sigma_r$ denote the distinct real embeddings $K \hookrightarrow \mathbb{R}$ and $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s$, the $2s$ complex embeddings $K \hookrightarrow \mathbb{C}$. Here, $\overline{\tau}(\alpha) := \overline{\tau(\alpha)}$, the composition of complex conjugation with τ. By definition, we must have $n = r + 2s$.

There is an additive group monomorphism $\Phi : K \hookrightarrow \mathbb{R}^n$ given by

$$\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \operatorname{Re}\tau_1(\alpha), \operatorname{Im}\tau_1(\alpha), \ldots, \operatorname{Re}\tau_s(\alpha), \operatorname{Im}\tau_s(\alpha)).$$

Before proceeding, fix an integral basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathfrak{o}$ over $\mathbb{Z}$.

LEMMA 2.4. $\Phi(\alpha_1), \ldots, \Phi(\alpha_n)$ are linearly independent over $\mathbb{R}$.

Proof. Let A be the matrix with i-th row as $\Phi(\alpha_i)$. First, subtract $i = \sqrt{-1}$ times the column corresponding to $\operatorname{Im}\tau_j$ from the column corresponding to $\operatorname{Re}\tau_j$. Then, multiply the column corresponding to τ_j by $2i$ and finally add the column corresponding to $\operatorname{Re}\tau_j$ to the column corresponding to $\operatorname{Im}\tau_j$. We then have

$$\det A = \frac{1}{(2i)^s} \det \begin{pmatrix} \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \sigma_1(\alpha_j) & \cdots & \sigma_r(\alpha_j) & \overline{\tau}_1(\alpha_j) & \tau_1(\alpha_j) & \cdots & \overline{\tau}_s(\alpha_j) & \tau_s(\alpha_j) \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \end{pmatrix}$$

In particular, this gives

$$|\det A| = \frac{1}{2^s}\sqrt{|d_K|} \neq 0,$$

where d_K is the discriminant of K. ∎

Before we proceed, we recall the Smith Normal Form for $\mathbb{Z}$. Let G be a free abelian group of rank n, and H a subgroup of G of finite index. The inclusion $H \hookrightarrow G$ is an injective homomorphism of free abelian groups having the same rank. This inclusion can be put into the Smith normal form, whence there is a basis $\{\gamma_1, \ldots, \gamma_n\}$ of H and $\{\beta_1, \ldots, \beta_n\}$ of G such that $\gamma_i = d_i\beta_i$ for $1 \leqslant i \leqslant n$, and $0 < d_1 \mid d_2 \mid \cdots \mid d_n$. It follows that $[G : H] = d_1 \cdots d_n$.

THEOREM 2.5. Let $\mathfrak{a}$ be a non-zero ideal of $\mathfrak{o}$. Then the image of $\mathfrak{a}$ under Φ in $\mathbb{R}^n$ is a complete lattice with fundamental parallelotope having (Lebesgue) volume

$$\operatorname{vol}\left(\mathbb{R}^n/\Phi(\mathfrak{a})\right)\frac{1}{2^s}\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|}$$

Proof. We can choose an integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathfrak{o}$ such that there are positive integers $d_1 \mid d_2 \mid \cdots \mid d_n$ such that $d_1\alpha_1, \ldots, d_n\alpha_n$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$. The image under Φ of this integral basis of $\mathfrak{a}$ is $d_1\Phi(\alpha_1), \ldots, d_n\Phi(\alpha_n)$. The volume of this parallelotope is precisely $d_1 \cdots d_n$ times the volume of the parallelotope we computed earlier, that is,

$$d_1 \cdots d_n \times \frac{1}{2^s}\sqrt{|d_k|} = \frac{1}{2^s}\mathfrak{N}(\mathfrak{a})\sqrt{|d_K|},$$

as desired. ∎

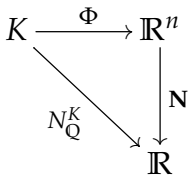
LEMMA 2.6 (MINKOWSKI). Let $\Lambda \subseteq \mathbb{R}^n$ be a complete lattice, and $E \subseteq \mathbb{R}^n$ a convex, measurable subset that is symmetric about 0 (equiv. centrally symmetric). If $\operatorname{vol}(E) > 2^n \operatorname{vol}\left(\mathbb{R}^n/\Lambda\right)$, then E contains a lattice point of Λ.
Further, if E is compact, then the same conclusion holds if $\operatorname{vol}(E) \geqslant 2^n \operatorname{vol}\left(\mathbb{R}^n/\Lambda\right)$.

Proof. ∎

Now, define a "norm map" $\mathbf{N} : \mathbb{R}^n \to \mathbb{R}$ by

$$\mathbf{N}(x) = x_1 \cdots x_r \left(x_{r+1}^2 + x_{r+2}^2\right) \cdots \left(x_{r+2s-1}^2 + x_{r+2s}^2\right).$$

It is not hard to see that there is a commutative diagram



COROLLARY 2.7. Let $A \subseteq \mathbb{R}^n$ be a compact, convex, centrally symmetric subset of $\mathbb{R}^n$ such that for each $x \in A$, $|\mathbf{N}(x)| \leqslant 1$. Then, every complete lattice Λ in $\mathbb{R}^n$ contains a non-zero point x with

$$|\mathbf{N}(x)| \leqslant \frac{2^n}{\operatorname{vol}(A)} \operatorname{vol}\left(\mathbb{R}^n/\Lambda\right).$$

Proof. Let $t > 0$ be such that

$$t^n = \frac{2^n}{\operatorname{vol}(A)} \operatorname{vol}\left(\mathbb{R}^n/\Lambda\right),$$

and set $E = tA$. Then, $\operatorname{vol}(E) = 2^n \operatorname{vol}\left(\mathbb{R}^n/\Lambda\right)$. Since E is compact, Lemma 2.6 implies the existence of a non-zero $x \in \Lambda \cap E$. Then $x = ta$ for some $a \in A$. As a result,

$$|\mathbf{N}(x)| = t^n \, |\mathbf{N}(a)| \leqslant t^n,$$

as desired. ∎

THEOREM 2.8. Every full lattice $\Lambda \subseteq \mathbb{R}^n$ contains a non-zero point $x \in \Lambda$ with

$$|\mathbf{N}(x)| \leqslant \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^s \operatorname{vol}\left(\mathbb{R}^n/\Lambda\right).$$

Proof. Let

$$A = \left\{ x \in \mathbb{R}^n \colon |x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leqslant n \right\}.$$

Then A is compact and for each $x \in A$, due to the AM-GM inequality, it follows that $|\mathbf{N}(x)| \leqslant 1$. It also follows from the triangle inequality that A is convex. In order to invoke the preceding result, we must compute the volume of A.

Let $V_{r,s}(t)$ denote the volume of

$$A_{r,s}(t) = \left\{ x \in \mathbb{R}^n \colon |x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leqslant t \right\},$$

where $n = r + 2s$. Then, $V_{r,s}(t) = t^{r+2s} V_{r,s}(1)$, and note that for $r \geqslant 1$,

$$V_{r,s}(1) = 2\int_0^1 V_{r-1,s}(1-x)\, dx = 2V_{r-1,s}(1)\int_0^1 (1-x)^{r+2s-1}\, dx = \frac{2}{r+2s} V_{r-1,s}(1).$$

Inducting downwards, this gives

$$V_{r,s}(1) = \frac{2^r (2s)!}{(r+2s)!} V_{0,s}(1).$$

Again, if $s \geqslant 1$, then

$$\begin{aligned}
V_{0,s}(1) &= \iint_{B\left(0,\frac{1}{2}\right)} V_{0,s-1}\left(1 - 2\sqrt{x^2+y^2}\right)\, dxdy \\
&= V_{0,s-1}(1) \iint_{B\left(0,\frac{1}{2}\right)} \left(1 - 2\sqrt{x^2+y^2}\right)^{2(s-1)}\, dxdy \\
&= V_{0,s-1}(1) \int_0^{2\pi} \int_0^{\frac{1}{2}} (1-2r)^{2(s-1)}\, r\, drd\theta \\
&= 2\pi V_{0,s-1}(1) \int_0^{\frac{1}{2}} (1-2r)^{2(s-1)} r\, dr \\
&= \frac{\pi}{2} V_{0,s-1}(1) \int_0^1 (1-t)^{2(s-1)} t\, dt \\
&= \frac{\pi}{2} V_{0,s-1}(1) \beta(2, 2s-1) \\
&= \frac{\pi}{2} \frac{\Gamma(2)\Gamma(2s-1)}{\Gamma(2s+1)} V_{0,s-1} \\
&= \frac{\pi}{2} \frac{1}{2s(2s-1)} V_{0,s-1}(1).
\end{aligned}$$

Inducting downwards, we obtain

$$V_{0,s}(1) = \left(\frac{\pi}{2}\right)^{s-1} \frac{1}{(2s)\cdot(2s-1)\cdot\cdots\cdot 3} V_{0,1}(1) = \left(\frac{\pi}{2}\right)^{s} \frac{1}{(2s)!}.$$

Thus,

$$\mathrm{vol}(A) = n^n V_{r,s}(1) = n^n \frac{2^r (2s)!}{n!} \cdot \left(\frac{\pi}{2}\right)^{s} \frac{1}{(2s)!} = \frac{2^r \cdot n^n}{n!} \left(\frac{\pi}{2}\right)^{s}.$$

Finally, invoking the preceding corollary, we have our desired conclusion. ■

COROLLARY 2.9. Every non-zero integral ideal $\mathfrak{a}$ of $\mathfrak{o}$ contains a non-zero α such that

$$\left|N_{\mathbb{Q}}^{K}(\alpha)\right| \leqslant \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{s} \sqrt{|d_K|}$$

Proof. Let $\Lambda = \Phi(\mathfrak{a})$, a complete lattice in $\mathbb{R}^n$ and due to Theorem 2.5, we know that

$$\mathrm{vol}(\mathbb{R}^n/\Lambda) = \frac{1}{2^s} \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|}.$$

Combining this with the preceding corollary, we get that Λ contains a non-zero point $x = \Phi(\alpha)$ with

$$|N_{\mathbb{Q}}^{K}(\alpha)| = |\mathbf{N}(x)| \leqslant \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^{s} \cdot \frac{1}{2^s} \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|} = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{s} \sqrt{|d_K|},$$

as desired. ■

COROLLARY 2.10 (MINKOWSKI'S BOUND). Every ideal class in $\mathrm{Cl}(K)$ contains an integral ideal $\mathfrak{a}$ such that

$$\mathfrak{N}(\mathfrak{a}) \leqslant \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{s} \sqrt{|d_K|}.$$

Proof. Follows immediately from the preceding corollary and Corollary 2.2. ■

§§ Dirichlet's Unit Theorem

LEMMA 2.11. For any positive integers m and M, the set of algebraic integers α such that

- the degree of α is $\leqslant m$, and
- $|\alpha'| \leqslant M$ for all conjugates α' of α

is finite.

Proof. ■

§3 Valuation Theory

§§ Valuations

Definition 3.1. A *valuation* of a field K is a function $|\cdot| : K \to \mathbb{R}$ such that

- $|x| \geqslant 0$, and $|x| = 0$ if and only if $x = 0$,
- $|xy| = |x||y|$, and
- $|x + y| \leqslant |x| + |y|$

for all $x, y \in K$. We tacitly exclude the case where $|\cdot|$ is the trivial valuation, that is, $|x| = 1$ for all $x \in K^\times$.

Obviously, every valuation defines a natural metric on the field given by

$$d(x, y) = |x - y| \qquad \forall\, x, y \in K.$$

Definition 3.2. Two valuation of K are said to be *equivalent* if they define the same topology on K.

Proposition 3.3. Two valuations $|\cdot|_1$ and $|\cdot|_2$ on K are equivalent if and only if there exists a real number $s > 0$ such that

$$|x|_1 = |x|_2^s \qquad \forall\, x \in K.$$

Proof. If $|\cdot|_1 = |\cdot|_2^s$ for some $s > 0$, then it is obvious that they define the same topology on K. Now, for any valuation $|\cdot|_1$, the inequality $|x| < 1$ is equivalent to the condition that $\{x^n : n \in \mathbb{N}\}$ converges to 0 in the topology defined by $|\cdot|$. Therefore, if $|\cdot|_1$ and $|\cdot|_2$ are equivalent, one has the implication

$$|x|_1 < 1 \implies \{x^n : n \in \mathbb{N}\} \text{ converges to } 0 \implies |x|_2 < 1.$$

Analogously, one has an implication in the other direction. That is, $|x|_1 < 1$ if and only if $|x|_2 < 1$.

Let $y \in K$ be fixed such that $|y|_1 > 1$. Let $x \in K$, $x \neq 0$. Then $|x|_1 = |y|_1^\alpha$ for some $\alpha \in \mathbb{R}$. Let $\{m_i/n_i\}$ be a sequence of rational numbers (with $n_i > 0$) converging to α from above. Then we have $|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i}$. Hence

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_1 < 1 \implies \left|\frac{x^{n_i}}{y^{m_i}}\right| < 1,$$

so that $|x|_2 < |y|_2^{m_i/n_i}$, and thus $|x|_2 \leqslant |y|_2^\alpha$ as we let $i \to \infty$. Similarly, taking a sequence of rationals converging to α from below, we get $|x|_2 \geqslant |y|_2^\alpha$. Thus, for all $x \in K$, $x \neq 0$, we get

$$\frac{\log |x|_1}{\log |x|_2} = \frac{\alpha \log |y|_1}{\alpha \log |y|_2} = \frac{\log |y|_1}{\log |y|_2} =: s > 0,$$

thereby completing the proof. ∎

THEOREM 3.4 (APPROXIMATION THEOREM). Let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent valuations of the field K and let $a_1, \ldots, a_n \in K$. Then for every $\varepsilon > 0$ there is an $x \in K$ such that

$$|x - a_i|_i < \varepsilon \quad \text{for all } 1 \leqslant i \leqslant n.$$

Proof. The theorem is obvious for $n = 1$, so we suppose that $n \geqslant 2$. Since $|\cdot|_1$ and $|\cdot|_n$ are inequivalent, there exist $\alpha, \beta \in K^\times$ such that $|\alpha|_1 < 1$, $|\alpha|_n \geqslant 1$, $|\beta|_1 \geqslant 1$, and $|\beta|_n < 1$. Setting $y = \beta/\alpha$, we get that $|y|_1 > 1$ and $|y|_n < 1$.

We shall prove by induction on n that there is a $z \in K$ such that

$$|z|_1 > 1 \quad \text{and} \quad |z|_j < 1 \quad \text{for } 2 \leqslant j \leqslant n.$$

We just proved this for $n = 2$, so suppose that $n \geqslant 3$ and assume we have found such a z for $2 \leqslant j \leqslant n-1$. If $|z|_n \leqslant 1$, then $z^m y$ will do for m sufficiently large. However, if $|z|_n > 1$, then the sequence $t_m = z^m/(1+z^m)$ converges to 1 with respect to $|\cdot|_1$ and $|\cdot|_n$, and to 0 with respect to $|\cdot|_2, \ldots, |\cdot|_{n-1}$ because

$$\left|1 - \frac{z^m}{1+z^m}\right|_i = \frac{1}{|1+z^m|_i} \leqslant \frac{1}{|z|_i^m - 1} \to 0$$

for $i \in \{1, n\}$ and

$$\left|\frac{z^m}{1+z^m}\right|_i = \frac{|z|_i^m}{|1+z^m|_i} \leqslant \frac{|z|_i^m}{1-|z|_i^m} \to 0$$

for $2 \leqslant i \leqslant n-1$. Hence, for sufficiently large m, $t_m y$ will suffice. Replace z with this newly found element. Note that the sequence $z^m/(1+z^m)$ converges to 1 with respect to $|\cdot|_1$ and to 0 with respect to $|\cdot|_2, \ldots, |\cdot|_n$. Therefore, we can choose z such that $|z|_1$ is as close to 1 as we like and $|z|_2, \ldots, |z|_n$ are as close to 0 as we like.

For each $1 \leqslant i \leqslant n$, choose a $z_i \in K$ as above (with 1 replaced by i) and finally set $x = a_1 z_1 + \cdots + a_n z_n$. We have

$$|x - a_i|_i \leqslant |a_1|_i |z_1|_1 + \cdots + |a_i||z_i - 1|_i + \cdots + |a_n|_i |z_n|_i.$$

Due to the preceding paragraph the z_i's can be chosen such that $|x - a_i| < \varepsilon_i$ for $1 \leqslant i \leqslant n$. This completes the proof. ∎

DEFINITION 3.5. A valuation $|\cdot|$ is called *non-archimedean* if $\{|n| : n \in \mathbb{N}\}$ is bounded. Otherwise, it is called *archimedean*.

PROPOSITION 3.6. A valuation $|\cdot|$ is non-archimedean if and only if it satisfies the *ultrametric inequality*

$$|x + y| \leqslant \max\{|x|, |y|\} \quad \text{for } x, y \in K.$$

Proof. If $|\cdot|$ satisfies the ultrametric inequality, then

$$|n| = |1 + \cdots + 1| \leqslant |1| = 1,$$

as desired. Conversely, suppose $|\cdot|$ is non-archimedean and let $|x| \geqslant |y|$ and $M > 0$ be such that $|n| \leqslant M$ for all $n \in \mathbb{N}$. We then have

$$|x+y|^n = \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \leqslant M \sum_{k=0}^{n} |x|^k |y|^{n-k} \leqslant N(n+1)|x|^n.$$

Taking n-th roots, we have $|x+y|^n \leqslant N^{1/n}(n+1)^{1/n}|x|$. In the limit $n \to \infty$, we have $|x+y| \leqslant |x|$, as desired. ■

REMARK 3.7. If $|\cdot|$ is a non-archimedean valuation, and $x, y \in K$ with $|x| > |y|$, then we have

$$|x+y| \leqslant |x| \quad \text{and} \quad |x| = |(x+y)+(-y)| \leqslant \max\{|x+y|, |y|\} = |x+y|,$$

whence $|x+y| = |x|$, that is, $|x+y| = \max\{|x|, |y|\}$ whenever $|x| \neq |y|$.

THEOREM 3.8 (OSTROWSKI). Every valuation of $\mathbb{Q}$ is equivalent to one of the valuatiosn $|\cdot|_p$ or $|\cdot|_\infty$.

Proof. ■

§§ Hensel's Lemma

DEFINITION 3.9. Let K be a complete non-archimedean valued field with valuation ring $(\mathfrak{o}, \mathfrak{p}, \kappa)$. We call a polynomial $f(X) = a_0 + \cdots + a_n X^n \in \mathfrak{o}[X]$ *primitive* if $f(X) \not\equiv 0 \pmod{\mathfrak{p}}$. That is,

$$|f| := \max\{|a_0|, \ldots, |a_n|\} = 1.$$

LEMMA 3.10 (HENSEL'S LEMMA). Let K be a complete non-archimedean valued field with valuation ring $(\mathfrak{o}, \mathfrak{p}, \kappa)$. If a primitive polynomial $f(X) \in \mathfrak{o}[X]$ admits modulo $\mathfrak{p}$ a factorization

$$f(X) \equiv \overline{g}(X)\overline{h}(X) \bmod \mathfrak{p},$$

into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[X]$, then $f(X)$ admits a factorization $f(X) = g(X)h(X)$ into polynomials $g, h \in \mathfrak{o}[X]$ such that $\deg g = \deg \overline{g}$, and

$$g(X) \equiv \overline{g}(X) \bmod \mathfrak{p} \quad \text{and} \quad h(X) \equiv \overline{h}(X) \bmod \mathfrak{p}.$$

Proof. Let $d = \deg f$ and $m = \deg \overline{g}$. Then $m + \deg \overline{h} = \deg \overline{f} \leqslant d$. Let $g_0, h_0 \in \mathfrak{o}[X]$ be polynomials such that $g_0 \equiv \overline{g} \bmod \mathfrak{p}$, $h_0 \equiv \overline{h} \bmod \mathfrak{p}$, $\deg g_0 = m$, and $\deg h_0 \leqslant d - m$. Since $(\overline{g}, \overline{h}) = 1$, there are polynomials $a(X), b(X) \in \mathfrak{o}[X]$ satisfying $ag_0 + bh_0 \equiv 1 \bmod \mathfrak{p}$. Among the coefficients of the two polynomials $f - g_0h_0, ag_0 + bh_0 - 1 \in \mathfrak{p}[X]$, choose the one with largest absolute value $|\cdot|$, and call it π (not to be confused with the uniformizer).

We inductively look for polynomials of the form

$$g = g_0 + p_1\pi + p_2\pi^2 + \cdots \quad \text{and } h = h_0 + q_1\pi + q_2\pi^2 + \cdots,$$

where $p_i, q_i \in \mathfrak{o}[X]$ are such that $\deg p_i < m$, and $\deg q_i \leqslant d - m$. Let

$$g_{n-1} = g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1} \quad \text{and} \quad h_{n-1} = h_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1}.$$

Since K is complete, it is easy to see that the coefficients of g_n and h_n converge. Further, we have $f \equiv g_{n-1}h_{n-1} \bmod \pi^n$, whence, in the limit, $n \to \infty$, we would have $f = gh$. Thus, it only remains to construct the p_n's and q_n's.

We have already established g_0, h_0. Suppose now that $n \geqslant 1$. Then, in view of the relation

$$g_n = g_{n-1} + p_n\pi^n, \qquad h_n = h_{n-1} + q_n\pi^n,$$

the condition $f \equiv g_n h_n \bmod \pi^{n+1}$ is equivalent to

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\,\pi^n \bmod \pi^{n+1}.$$

Set $f_n = \pi^{-n}\,(f - g_{n-1}h_{n-1})$, then the above condition is equivalent to

$$f_n \equiv g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \bmod \pi.$$

Recall that $g_0a + h_0b \equiv 1 \bmod \pi$ due to our choice of π, and hence,

$$g_0af_n + h_0bf_n \equiv f_n \bmod \pi.$$

Next, we write

$$b(X)f_n(X) = q(X)g_0(X) + p_n(X),$$

in $K[X]$, where $\deg p_n < \deg g_0 = m$. Since $g_0 \equiv \overline{g} \bmod \mathfrak{p}$, and $\deg g_0 = \deg \overline{g}$, the leading term of g_0 is a unit, whence $q(X), p_n(X) \in \mathfrak{o}[X]$. We obtain the congruence,

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \bmod \pi.$$

Omit from the polynomial $a(X)f_n(X) + h_0(X)q(X)$ all coefficients that are divisible by π to get a polynomial $q_n(X)$ such that $g_0q_n + h_0p_n \equiv f_n \bmod \pi$.

Finally, note that $\deg f_n \leqslant d$, $\deg g_0 = m$, and $\deg(h_0p_n) < (d-m) + m = d$. Hence, g_0q_n has degree $\leqslant d$ modulo π. Recall that the leading coefficient of g_0 is a unit in $\mathfrak{o}$, and the leading coefficient of q_n is not divisible by π, and hence, the degree of $g_0(X)q_n(X)$ modulo π is precisely $m + \deg q_n$, whence $\deg q_n \leqslant d - m$. This completes the induction step, and hence, the proof. ■

COROLLARY 3.11. Let K be complete with respect to the non-archimedean valuation $|\cdot|$. Then, for every irreducible polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ with $a_0a_n \neq 0$, one has

$$|f| = \max\{|a_0|, |a_n|\}.$$

In particular, $a_n = 1$ and $a_0 \in \mathfrak{o}$ imply that $f \in \mathfrak{o}[X]$.

Proof. Multiplying by a suitable element of K, we may suppose that $f \in \mathfrak{o}[X]$, and $|f| = 1$. Let $r \geqslant 0$ be the smallest such that $|a_r| = 1$. That is, we have

$$f(X) \equiv X^r\left(a_r + a_{r+1}X + \cdots + a_nX^{n-r}\right) \bmod \mathfrak{p}.$$

If $\max\{|a_0|, |a_n|\} < 1$, then $0 < r < n$, and hence, due to Hensel's Lemma, could lift the above factorization a non-trivial factorization in $\mathfrak{o}[X]$, contradicting the irreducibility of $f(X) \in K[X]$. This completes the proof. ■

THEOREM 3.12. Let K be complete with respect to the valuation $|\cdot|$, and suppose L/K is an algebraic extension. Then, there is a unique extension of $|\cdot|$ to L. Further, if L is finite over K, then the extension is given by

$$|\alpha| = \sqrt[n]{\left|N_K^L(\alpha)\right|},$$

and L is also complete.

Proof. Suppose we have shown the second assertion of the theorem, that is, for every finite extension L/K, there is a unique extension of $|\cdot|$ to L given by the above formula. We can then extend this valuation to all of $\overline{K}$ (the algebraic closure of K) by defining

$$|\alpha| = \sqrt[n]{\left|N_K^L(\alpha)\right|} \qquad n = [L:K],$$

and L is any finite extension of K containing α. First, we note that this is well-defined. Indeed, if $m = [K(\alpha):K]$, then

$$N_K^L(\alpha) = N_K^{K(\alpha)}\left(N_{K(\alpha)}^L(\alpha)\right) = \left(N_K^{K(\alpha)}(\alpha)\right)^{[L:K(\alpha)]},$$

consequently,

$$|\alpha| = \sqrt[m]{\left|N_K^{K(\alpha)}(\alpha)\right|},$$

which is independent of our choice of finite extension L/K. Further, since the extension of $|\cdot|$ to every finite subextension of $\overline{K}$ is unique, and K is the union of all such subextensions, we see that there is a unique extension of $|\cdot|$ to $\overline{K}$.

All that remains is to argue for the existence and uniqueness of an extension of $|\cdot|$ to L where L/K is a finite extension with $n = [L:K]$.

- **Existence:** Let $(\mathfrak{o}, \mathfrak{p}, \kappa)$ be the valuation ring of K and $\mathfrak{O}$ its integral closure in L. We claim that
$$\mathfrak{O} = \left\{\alpha \in L \colon N_K^L(\alpha) \in \mathfrak{o}\right\}.$$
Indeed, if $\alpha \in \mathfrak{O}$, then $N_K^L(\alpha)$ is integral over $\mathfrak{o}$ and lies in K, and hence it lies in $\mathfrak{o}$, since $\mathfrak{o}$ is integrally closed in K. Conversely, suppose $\alpha \in L^\times$ is such that $N_K^L(\alpha) \in \mathfrak{o}$. Let
$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$$
be the minimal polynomial of α over K. Then $N_K^L(\alpha) = \pm a_0^m \in \mathfrak{o}$, and hence, $|a_0| \leqslant 1$. Then, due to Corollary 3.11, we see that $f(X) \in \mathfrak{o}[X]$, that is, $\alpha \in \mathfrak{O}$. This proves our claim.

  All that remains to show is that the function $|\alpha| = \sqrt[n]{\left|N_K^L(\alpha)\right|}$ satisfies the ultrametric inequality. Indeed, suppose $|\alpha| \leqslant |\beta|$ and $\beta \neq 0$. We want to show that $|\alpha + \beta| \leqslant \max\{|\alpha|, |\beta|\}$, which, after dividing throughout by β, is equivalent to showing $|\alpha + 1| \leqslant \max\{|\alpha|, 1\}$, whenever $|\alpha| \leqslant 1$. Note that $|\alpha| \leqslant 1$ implies $\left|N_K^L(\alpha)\right| \leqslant 1$, whence, due to the preceding paragraph, $\alpha \in \mathfrak{O}$. Since $\mathfrak{O}$ is a ring, we see that $\alpha + 1 \in \mathfrak{O}$, and again, due to the preceding paragraph, we must have $|\alpha + 1| \leqslant 1$. This completes the proof of existence.

- **Uniqueness:** Let $|\cdot|'$ be another extension with valuation ring $(\mathfrak{O}', \mathfrak{P}')$. We claim that $\mathfrak{O} \subseteq \mathfrak{O}'$. Suppose not, and choose $\alpha \in \mathfrak{O} \setminus \mathfrak{O}'$, and let

  $$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathfrak{o}[X]$$

  be the minimal polynomial of α over K. Then, one has $\alpha^{-1} \in \mathfrak{P}'$, since $|\alpha|' > 1$. Hence,

  $$1 = -a_1\alpha^{-1} - \cdots - a_d \left(\alpha^{-1}\right)^d \in \mathfrak{P}',$$

  a contradiction. This shows that inclusion $\mathfrak{O} \subseteq \mathfrak{O}'$, which is equivalent to the statement

  $$|\alpha| \leqslant 1 \implies |\alpha|' \leqslant 1,$$

  whence the two valuations are equivalent on L, and hence, $|\cdot| = |\cdot|^s$ for some $s > 0$. But since the two valuations agree on K, we must have $s = 1$, that is, $|\cdot| = |\cdot|'$. This completes the proof. ∎

Lemma 3.13 (Krasner). Let $(K, |\cdot|)$ be a complete valued field, $\alpha \in K^{sep}$ and $\beta \in \overline{K}$. Let $\alpha_1, \ldots, \alpha_n$ be the distinct conjugates of α in $\overline{K}$ with $\alpha \neq \alpha_i$ for $1 \leqslant i \leqslant n$. If

$$|\alpha - \beta| < |\alpha - \alpha_i| \qquad \forall\, 1 \leqslant i \leqslant n,$$

then $K[\alpha] \subseteq K[\beta]$.

Proof. Suppose $K[\alpha] \not\subseteq K[\beta]$. Since α is separable over $K[\beta]$, there is an automorphism $\sigma \in \mathrm{Aut}(\overline{K}/K[\beta])$ such that $\sigma\alpha \neq \alpha$ but $\sigma\beta = \beta$. ∎

Theorem 3.14. Let $(K, |\cdot|)$ be a complete field. If L/K is an infinite separable algebraic extension, then L is not complete.

Proof. If $|\cdot|$ were archimedean, then $K = \mathbb{R}$ or $K = \mathbb{C}$, neither of which admit infinite degree algebraic extensions. Thus, we may suppose that $|\cdot|$ is non-archimedean. We have seen that there is a unique extension of $|\cdot|$ to $\overline{K}$ which we shall denote by $|\cdot|$ too. Suppose $(L, |\cdot|)$ is complete. Let $x_0, x_1, x_2, \ldots$ be a K-linearly independent subset of L. We shall construct a sequence $\{a_n\}_{n \geqslant 0}$ of non-zero elements in K such that:

(1) $|a_n x_n| \to 0$ monotonically as $n \to \infty$.

(2) If we set

$$s_n = a_0 x_0 + \cdots + a_{n-1} x_{n-1} \qquad n \geqslant 1,$$

then

$$|a_n x_n| < d_n = \min\{|s_n - \sigma s_n| \colon \sigma \in \mathrm{Gal}(K^{sep}/K)\} \setminus \{0\}.$$

This is achieved inductively, using the fact that K contains elements of arbitrarily small valuation, indeed choose any $\alpha \in K$ with $|\alpha| < 1$ and take α^m for sufficiently large m. Since we are in a non-archimedean field the sequence $\{s_n\}$ is Cauchy, and converges to some $s \in K$. The ultrametric inequality then gives

$$|s_n - s| = \left|\sum_{k=n}^{\infty} a_k x_k\right| = |a_n x_n| < d_n,$$

whence, due to Krasner's Lemma, $s_n \in K(s)$ for all $n \geqslant 1$. But since the s_n's are linearly independet, we see that $[K(s) : K] = \infty$, which is absurd. Thus, L cannot be complete. ■

REMARK 3.15. In particular, $\overline{\mathbb{Q}}_p$ is not complete and hence, admits a proper completion which we denote by $\mathbb{C}_p$.

THEOREM 3.16. Let $(K, |\cdot|)$ be a complete valued field and as we have seen the valuation on K extends uniquely to $\overline{K}$. Then, the completion $\mathbb{C}_K$ of $\overline{K}$ under this valuation is algebraically closed.

Proof. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}_K[X]$. Since $\overline{K}$ is dense in $\mathbb{C}_K$, we can choose $a_{i,j} \in \overline{K}$ such that

- $|a_{i,j} - a_i| < \min\left\{|a_i|, \frac{1}{j}\right\}$ if $a_i \neq 0$, and
- $a_{i,j} = 0$ if $a_i = 0$.

Hence, $|a_{i,j}| = |(a_{i,j} - a_i) + a_i| = |a_i|$. Set

$$f_j(X) = X^n + a_{n-1,j}X^{n-1} + \cdots + a_{0,j} \in \overline{K}[X].$$

Pick any root $r_j \in \overline{K}$ of $f_j(X)$. We shall show that the sequence $\{r_j\}$ admits a convergent subsequence. First, note that

$$|r_j|^n = \left|\sum_{i=0}^{n-1} a_{i,j} r_j^i\right| = \max_{0 \leqslant i \leqslant n-1} |a_i||r_j|^i = |a_{i(j)}||r_j|^{i(j)},$$

for some $0 \leqslant i(j) \leqslant n-1$. In particular, this gives

$$|r_j| \leqslant |a_{i(j)}|^{\frac{1}{n-i(j)}},$$

that is,

$$|r_j| \leqslant C := \max_{0 \leqslant i \leqslant n-1} |a_i|^{\frac{1}{n-i}}.$$

Now,

$$|f(r_j)| = |f(r_j) - f_j(r_j)| = \left|\sum_{i=0}^{n-1} (a_i - a_{i,j}) r_j^i\right| \leqslant \max_{0 \leqslant i \leqslant n-1} |a_i - a_{i,j}||r_j|^i.$$

Note that if $C \geqslant 1$, then $|r_j|^i \leqslant C^i \leqslant C^{n-1}$ and if $C < 1$, then $|r_j|^i < 1$. In particular, we have $|r_j|^i \leqslant \max\{1, C^{n-1}\}$, thus

$$|f(r_j)| \leqslant \max_{0 \leqslant i \leqslant n-1} |a_i - a_{i,j}| \cdot \max\{1, C^{n-1}\} \leqslant \frac{\max\{1, C^{n-1}\}}{j},$$

that is, $f(r_j) \to 0$ as $j \to \infty$. Let $L \supseteq \mathbb{C}_K$ be a splitting field of $f(X)$ and extend the absolute value $|\cdot|$ on $\mathbb{C}_K$ to L. Then, we can write $f(X) = (X-\rho_1)\cdots(X-\rho_n)$ for some $\rho_1, \ldots, \rho_n \in L$. Then,

$$\lim_{j\to\infty} \prod_{k=1}^{n} |r_j - \rho_k| = 0.$$

Suppose none of the sequences $\{|r_j - \rho_k|\}_{j=1}^{\infty}$ admit convergent subsequences, then for every $1 \leqslant k \leqslant n$, there is an $\varepsilon_k > 0$ such that $|r_j - \rho_k| \geqslant \varepsilon_k$ for all $j \geqslant N_k$. Therefore,

$$\prod_{k=1}^{n} |r_j - \rho_k| \geqslant \varepsilon_1 \cdots \varepsilon_n$$

for all $j \geqslant \max\{N_1, \ldots, N_k\}$, a contradiction. Suppose k_0 is such that $\{|r_j - \rho_{k_0}|\}_{j=1}^{\infty}$ admits a convergent subsequence, then $\{r_j\}$ admits a convergent subsequence converging to ρ_{k_0}. This shows that $\{r_j\}$ admits a Cauchy subsequence $\{r_{j_i}\}_{i=1}^{\infty}$ in $\mathbb{C}_K$, which converges to some $r \in \mathbb{C}_K$. Then,

$$f(r) = \lim_{j\to\infty} f_{j_i}(r_{j_i}) = 0,$$

since the coefficients of f_j converge to those of f as $j \to \infty$. This shows that $\mathbb{C}_K$ is algebraically closed, thereby completing the proof. ■

Remark 3.17. In particular, $\mathbb{C}_p$ is algebraically closed.

Theorem 3.18. Let $(K, |\cdot|)$ be a complete valued field and let V be an n-dimensional normed vector space over K. Then for any basis $v_1, \ldots, v_n$ of V, the maximum norm

$$\|x_1 v_1 + \cdots + x_n v_n\| = \max\{|x_1|, \ldots, |x_n|\}$$

is equivalent to the given norm on V. In particular, V is complete and the isomorphism

$$K^n \longrightarrow V \qquad (x_1, \ldots, x_n) \longmapsto x_1 v_1 + \cdots + x_n v_n$$

is a homeomorphism.

Proof. ■

Corollary 3.19. Let X be a normed linear space over a complete valued field $(K, |\cdot|)$. Every finite-dimensional subspace of X is closed in X.

Proof. Due to Theorem 3.18, the finite-dimensionaln subspace is a complete subspace of a metric space, and hence, is closed. ■

§§ Local Fields

Definition 3.20. A complete discretely valued field having finite residue class field is called a *local field*.

THEOREM 3.21. Let $(K, |\cdot|)$ be a non-archimedean valued field with valuation ring $(\mathfrak{o}, \mathfrak{p}, \kappa)$. Then $\mathfrak{o}$ is compact if and only if $|\cdot|$ is discrete, complete, and κ is finite (i.e. K is a local field).

Proof. Suppose $\mathfrak{o}$ is compact. We first show that K is complete. Suppose (x_n) is a Cauchy sequence in K. Then, there is an $N \in \mathbb{N}$ such that for all $m, n \geqslant N$, $|x_m - x_n| \leqslant 1$ whenever $m, n \geqslant N$. In particular, $|x_n - x_N| \leqslant 1$ whenever $n \geqslant N$. Since $\mathfrak{o}$ is a compact metric space, it is complete, and the sequence $(x_n - x_N)_{n \geqslant N}$ is Cauchy, so it converges to some $y \in \mathfrak{o}$. It follows that the sequence (x_n) converges to $x_N + y \in K$.

Since $\mathfrak{p}$ is open in $\mathfrak{o}$, it must have finite index, else the cosets of $\mathfrak{p}$ in $\mathfrak{o}$ would form an infinite open cover consisting of disjoint open sets, which obviously does not admit a finite subcover. Thus κ is finite.

Finally, since $\mathfrak{p}$ is finite index and open in $\mathfrak{o}$, it must be closed, whence compact. Let $z_0 \in \mathfrak{p}$ be the point maximizing $|\cdot|$ on $\mathfrak{p}$. Since $|z_0| < 1$ and there is no $z \in K$ such that $|z_0| < z < 1$, we see that $|\cdot|$ is discrete.

Conversely, suppose $|\cdot|$ is discrete, complete, and κ is finite. Since $\mathfrak{o}$ is closed in K, it is complete too. We shall show that $\mathfrak{o}$ is totally bounded, whence compactness would follow. Let $\varepsilon > 0$, π be the uniformizer of $|\cdot|$, and choose n sufficiently large so that $|\pi^n| < \varepsilon$, then each coset $x + \pi^n\mathfrak{o}$ has diameter equal to that of $\pi^n\mathfrak{o}$, whose diameter is

$$\sup_{x,y \in \mathfrak{o}} |\pi^n x - \pi^n y| = |\pi^n| \sup_{x,y \in \mathfrak{o}} |x - y| \leqslant |\pi^n| < \varepsilon.$$

Since $\mathfrak{o}/\pi^n\mathfrak{o}$ has finite cardinality, we have obtained an finite open cover of $\mathfrak{o}$ using balls of diameter at most ε, whence total boundedness follows, thereby completing the proof. ∎

COROLLARY 3.22. Let $(K, |\cdot|)$ be a non-archimedean valued field. Then K is a local field if and only if it is locally compact.

Proof. If K is a local field, then due to Theorem 3.21, $\mathfrak{o}$ is compact. Since every open set containing the origin contains a neighborhood of the form $B(0, \varepsilon)$ for some $\varepsilon < 1$, its closure is closed in $\mathfrak{o}$ and hence, is compact. It follows that K is locally compact.

Conversely, suppose K is locally compact. Then, there is compact set C containing 0 with non-empty interior. We may further suppose that 0 is contained in the interior. Thus, there is a $\varepsilon > 0$ such that $B(0, \varepsilon) \subseteq C$. Since C is closed, $\overline{B}(0, \varepsilon) \subseteq C$, so the former is compact. Choose $\alpha \in K$ such that $\varepsilon|\alpha| > 1$, then $\alpha \cdot \overline{B}(0, \alpha)$ is a compact set containing $\mathfrak{o} = \overline{B}(0, 1)$. Since the latter is closed, it must be compact, whence due to Theorem 3.21, K is a local field. This completes the proof. ∎

REMARK 3.23. We may, more generally, define $(K, |\cdot|)$ to be a local field if and only if K is locally compact. This also justifies the usage of the word "local". Indeed, as we have seen in the above proof, the local compactness of K implies the compactness of $\overline{B}(0, 1)$. This can then be used to show the completeness of K as in the proof of Theorem 3.21. Thus, if $(K, |\cdot|)$ were a locally compact archimedean valued field, then it must be a complete archimedean valued field, consequently K is either $\mathbb{R}$ or $\mathbb{C}$. On the other hand, if $(K, |\cdot|)$ is a locally compact non-archimedean valued field, then due to the above result, K is a local field in our sense.

DEFINITION 3.24. Let X be a normed linear space over a valued field $(K, |\cdot|)$. A subset $A \subseteq X$ is said to be *balanced* if $\alpha A \subseteq A$ whenever $|\alpha| \leqslant 1$.

In particular, the balls centered at 0 in X are balanced and this is the only example we shall need.

LEMMA 3.25. Let X be a topological vector space over a valued field $(K, |\cdot|)$ and (α_n) a sequence in K such that $|\alpha_n| \to \infty$ as $n \to \infty$. Then

$$X = \bigcup_{n=1}^{\infty} \alpha_n U.$$

Proof. Let $x \in X$. Since the multiplication map $K \times X \to X$ is continuous and $(0, x) \mapsto 0$, there is a neighborhood $B(0, \varepsilon)$ of 0 in K and an open neighborhood V of the origin such that $B(0, \varepsilon) \times (x + V) \mapsto U$. Choose α_n such that $|\alpha_n| > 1/\varepsilon$. Then $\alpha_n^{-1} x \in U$, whence $x \in \alpha_n U$, thereby completing the proof. ∎

LEMMA 3.26. Let X be a locally compact normed linear space over a complete valued field $(K, |\cdot|)$. Then X is finite-dimensional.

Proof. This argument is due to André Weil, reproduced in Rudin's *Functional Analysis*. Let $V \subseteq X$ be a relatively compact neighborhood of 0. We can suppose that V is a ball in X, in particular, V is balanced and relatively compact. Let (α_n) be a sequence in $K^\times$ converging to 0. We claim that the collection $\{\alpha_n V\}$ is a local base at 0. Due to the preceding lemma, $\{\alpha_n^{-1} U\}$ is an open cover of $\overline{V}$, whence admits a finite subcover $\{\alpha_{n_1}^{-1} U, \ldots, \alpha_{n_k}^{-1} U\}$. Choose α_{n_i} that maximizes $|\alpha_{n_j}|^{-1}$. Then $\overline{V} \subseteq \alpha_{n_i}^{-1} U$, that is, $\alpha_{n_i} V \subseteq U$, which proves our claim.

Finally, choose some $\alpha \in K$ with $|\alpha| \leqslant \frac{1}{2}$. Since $\overline{V}$ is compact, there are $x_1, \ldots, x_n \in \overline{V}$ such that $\overline{V} \subseteq (x_1 + \alpha V) \cup \cdots \cup (x_n + \alpha V)$. Let Y denote the linear subspace of X generated by $x_1, \ldots, x_n$. We have that

$$\overline{V} \subseteq Y + \alpha V \subseteq Y + \alpha (Y + \alpha V) = Y + \alpha^2 V,$$

and so on. Therefore,

$$\overline{V} \subseteq \bigcap_{n=1}^{\infty} (Y + \alpha^n V) = \overline{Y} = Y,$$

where the second-last equality follows from the fact that $\{\alpha^n V\}$ forms a basis of X and the last equality follows from the fact that finite-dimensional subspaces of a normed linear space are closed. Due to Lemma 3.25,

$$X = \bigcup_{n=1}^{\infty} \alpha^{-n} V \subseteq Y,$$

whence X is finite-dimensional. This completes the proof. ∎

THEOREM 3.27. The local fields are precisely the finite extensions of the fields $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.

Proof. ∎